# Operational Capabilities Demonstration Criteria for Shared Services Provider Candidates

## Introduction

The Federal government intends to identify and properly qualify Shared Service Provider (SSP) candidates who will provide PKI services and infrastructure to support a common PKI implementation for the Federal government. This document outlines the evaluation criteria, which is referred to as an Operational Capabilities Demonstration (OCD).

The Shared Service Provider Subcommittee (Subcommittee), operating at the direction of the Federal Identity Credentialing Committee (FICC), is tasked with establishing the criteria used by the Federal government to validate the acceptability of an SSP candidate. Actual evaluation of an SSP candidate will be accomplished in concert with the Federal Common Policy Working Group. After acceptance, on-going oversight is provided through the Federal PKI Policy Authority (FPKIPA), as provided for by the X.509 Certificate Policy for the Common Policy Framework (Federal Common Policy). This includes review and acceptance of the Certification Practice Statement (CPS) and compliance audits.

## Federal Common Policy

The Federal Common Policy is the Certificate Policy (CP) designated for the common government trust anchor. The root Certification Authority (CA) is operated by the FPKIPA. The root CA shall sign each subordinate CA operated by a SSP, which in turn will be used to provide PKI services to Federal agencies contracting for services on an individual basis. Consult the Federal Common Policy for additional details.

## OCD Prerequisites

The SSP candidate shall submit a written request for evaluation to the point of contact identified in the Federal announcement for SSP services. The request shall be accompanied by the documents described below, which will be reviewed by the government in the manner identified. When deemed initially acceptable, the Federal government will notify the SSP candidate and coordinate a date to initiate the OCD.

1. The SSP candidate shall submit a CPS for review. The FICC shall review the CPS in accordance with the FICC developed CP-CPS Analysis Matrix. The FICC may refer questions related to the proposed CPS back to the SSP candidate for clarification.
2. The SSP candidate shall submit a current compliance audit which demonstrates that the SSP candidate has the ability to successfully establish and operate a PKI solution. The standard for the compliance audit shall be identified, and the credentials of the compliance auditor shall also be presented.

3. The SSP candidate shall submit a system architecture diagram which is representative of the proposed PKI solution(s) being offered to the government.

The FICC will review the submission of the prerequisites, and determine if the SSP candidate has complied with all of the preliminary. When the prerequisites are deemed to be acceptable, the FICC will contact the SSP candidate to complete arrangements for the OCD evaluation.

## Demonstration Criteria

This section outlines the mandatory and optional requirements associated with an OCD evaluation by the Federal government. The FICC reserves the right to augment the OCD criteria based on the proposed architecture and approach identified by the SSP candidate. This includes validation of specific areas identified in the SSP candidate's CPS submission, as evaluated against the CP-CPS Analysis Matrix.

### Mandatory Requirements

1. Demonstrate support for in-person verification of applicant's identity as specified in the Federal Common Policy:
    a. Demonstrate the method by which the Registration Authority (RA) and CA communicate applicant identity information, authorization information, etc.
2. Demonstrate support for Government Smart Card Interoperability Specification (GSC-IS) compliant smart card users:
    a. Issue certificates for signature keys generated for a user on GSC-IS compliant smart cards.
    b. Certificate must comply with Certificate & CRL Profile, including AIA, and CDP extensions.
    c. Provide newly generated user certificate to user and import certificate onto smart card.
3. Distribute trust anchor certificate to an RA or a user.
4. Authenticate and process Certificate Revocation Requests.
5. Generate CRLs that comply with Certificate & CRL Profile.
6. Demonstration support for repository requirements:
    a. Post CA certificates in LDAP directory as specified in Repository Profile and matching AIA/SIA extensions.
    b. Post CRLs in LDAP directory as specified in Repository Profile and matching CDP extension.
    c. Post CA certificates on HTTP web server as specified in Repository Profile and matching AIA/SIA extensions.
    d. Post CRLs on HTTP web server as specified in Repository Profile and matching CDP extension.
7. Demonstrate paper and electronic archiving in accordance with Archive Requirements document.
8. Demonstrate CA key rollover.
9. After key rollover, perform the following actions:
    a. Issue new certificates.

b. Revoke one "new" certificates and one "old" certificate.
c. Generate valid X.509 CRL(s) for all currently unexpired certificates.

### Optional Requirements

1. Demonstrate support for trusted agent verification of applicant's identity as specified in CP.
2. Issue certificates to software users.
3. Issue certificates for devices.
4. Escrow and recover encryption keys.
5. Demonstrate support for repository requirements:
    a. Post user certificates in LDAP directory as specified in Repository Profile.

The FICC will notify the SSP candidate of any deficiencies that require further attention. The SSP candidate should expect to resolve any deficiencies through re-evaluation against the OCD criteria. This is initiated by contacting the FICC for scheduling.

## Determination of Acceptability

After successful completion of the OCD evaluation process, a formal Determination of Acceptability will be generated by the FICC. Where deemed appropriate by the FICC, operating limitations can be enforced using the two alternatives provided for below:

1. In the first alternative, the SSP candidate may be approved to provide services related to the generation of digital certificates used for identity and digital signature in accordance with the Federal Common Policy. However, such approval may specifically preclude encryption related certificates because the SSP candidate did not specifically request consideration or has not yet successfully demonstrated the ability to generate, escrow, maintain, and recover encryption certificates. In such cases, the Determination of Acceptability shall specifically identify the limitation to services under the Federal Common Policy.
2. In the second alternative, the SSP candidate has substantially completed the OCD, certain deficiencies have been noted, and the FICC has agreed to a formal remediation plan. In such cases, the FICC has a reasonable expectation that the SSP candidate will be able to address any and all specific deficiencies in a timely manner. However, the FPKIPA will not approve the CPS to operate under the Common Federal Policy until the FICC is satisfied with the status of remediation efforts.

When a Determination of Acceptability is generated by the FICC, a copy will be provided to the SSP candidate, the FPKIPA, and the FICC will make the approval known to Federal agencies in a manner identified by the FICC.